APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/643,630	08/21/2000	W. Olin Sibert	7451.0028-00	5386

7590	04/08/2004		EXAMINER	
			SHIN, KYUNG H	

FINNEGAN HENDERSON FARABOW
GARRETT & DUNNER LLP
1300 I Street NW
WASHINGTON, DC 20005-3315

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 04/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/643,630	SIBERT, W. OLIN
	Examiner	Art Unit
	Kyung H Shin	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2000*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers dated 8/11/2000.

2. Claims **1-21** are pending. Amended claims are **1, 7, 10, 11,** and **18.** Claims **6, 9, 17** are canceled. Claims **1, 11, 19** are **independent**.

Drawings

3. New corrected drawings are required in this application because drawings done by hands. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.   **Claims 1- 21** are rejected under 35 U.S.C. 102(e) as being unpatentable over

Ginter et al. (U.S. Patent No. 6, 427,140: Systems and Methods for Secure

Transaction Management and Electronic Rights Protection, File date - Sep. 3, 1999).

Regarding Claim 1, Ginter et al. discloses a secure processing unit (SPU) comprising

a) an internal memory unit; (see col. 65, lines 13-15; SPU 500 in this example

includes a single microprocessor 520 and a limited amount of memory configured

as ROM 532 and RAM 534.)

b) a processor; (see col. 65, lines 13-15; same as above (a))

c) tamper detection and response logic; (see col. 169, lines 32-36; A trusted

environment of the present invention implemented, in part, through the use of

tamper resistant semiconductor design, contains control logic, such as a

microprocessor, that securely executes VDE processes.)

d) an interface to external systems or components; (see col. 65, lines 29-34;

Additional or alternate dedicated paths 538 may connect microprocessor 520 to

the other components (e.g., encrypt/decrypt engine 522 via line 538a, real-time

clock 528 via line 538b, bus interface unit 530 via line 538c, DMA controller via line

538d, and memory management unit (MMU) 540 via line 538e).)

e) one or more buses for connecting the internal memory unit, the processor, the

tamper detection and response logic, and the interface to external systems and

components; (see col. 62, lines 8-18; A trusted environment of the present

invention implemented, in part, through the use of tamper resistant semiconductor

design, contains control logic, such as a microprocessor, that securely executes
VDE processes.)

f) a memory management unit; (see col. 65, lines 15-20; memory management unit
(MMU) 540.)

g) a level-one page table, the level-one page table including a plurality of level-one
page table entries, wherein the level-one page table entries each correspond to at
least one level-two page table, and wherein the level-one page table entries each
contain a predefined attribute, the predefined attribute being operable to indicate
to the memory management unit whether entries in a corresponding level-two
page table may designate certain predefined memory regions;

(Applicant describes, see Summary pg. 3, lines 18-20; *"The level-one page
table entries contain an attribute that indicates whether the entries in the
corresponding level-two page table may designate certain memory regions. Level-
two page tables that are not allowed to designate certain regions of memory may
be stored outside of the secure processing unit in external memory"*; and also see,
Detailed Description, pg 11, 'Ch. 3 SPU memory protection with MMU': *"MMU
translates virtual address to physical addresses... on the physical address values
resulting from that translation,...."* ; and *"Fig. 5, Virtual Address Translation =
multi-level page translation,... virtual address is divided into three parts:... in level-
one page table,... level-two page table , and ..memory page."* see Detailed
Description, pg 16, 'Ch. 3.3 Memory protection by Page Table Attribute', *"... ,*

processor security registers can be used to designate internal memory as critical,

but external memory (excesses by external bus) as non-critical....",)

(The functions of the MMU in Ginter et al. , 'Systems and Methods for

Secure Transaction Management and Elctronic Rights Protection', discuss below

are the same functions as applicant's claim limitations: see Ginter, col. 69, lines

9-28; MMU provides hardware support for memory management and virtual

memory management functions. MMU may also provide hardware-level support

functions related to memory management such as, for example, address

mapping.)

(see Ginter, col. 69, lines 35-50; In these cases, secure processing steps

performed by an SPU typically must be segmented into small, securely packaged

elements that may be "paged in" and "paged out" of the limited available internal

memory space. Memory external to an SPU 500 may not be secure. Since the

external memory may not be secure, SPU 500 may encrypt and cryptographically

seal code and other information before storing it in external memory. Similarly,

SPU 500 must typically decrypt code and other information obtained from,

external memory in encrypted form before processing (e.g., executing) based on

it.)

h) a plurality of processor security registers; (see col. 107, lines 25-26; swapped

process "context" information (e.g., the register set for the process when it is not

processing))

i) a tamper-resistant housing. (see col. 169, lines 28-31; within a secure enclosure,

such as a tamper resistant metal container or some form of a chip pack containing

multiple integrated circuit components)

Regarding Claim 2, a secure processing unit as in claim 1, in which the internal

memory unit includes;

(a) secure random access memory (RAM); (see col. 69, lines 26) ;

(b) secure non-volatile memory (NVRAM); (see col. 70, lines 40-44);

(c) secure read-only memory (ROM) (see col. 69, lines 25).

Regarding Claim 3, a secure processing unit as in claim 2, in which the secure non-

volatile memory is powered by a battery. (see col. 70, lines 45-47; NVRAM ("non-

volatile RAM") 534b. RAM 534a may be volatile, while NVRAM 534b is preferably

battery backed)

Regarding Claim 4, a secure processing unit as in claim 3, in which the secure non-

volatile memory contains at least one cryptographic key. (see col. 70, lines 54-63;

certain highly sensitive information (e.g., certain load modules and certain encryption

key related information such as internally generated private keys) .... (NVRAM) 534b

may be used for securely storing such highly sensitive information)

Regarding Claim 5, a secure processing unit as in claim 1, in which the internal

memory unit includes a unique identifier for the secure processing unit, a private

cryptographic key, a public cryptographic key, and a cryptographic certificate linking

the unique identifier and the public cryptographic key. (see col. 120, lines 43-56; The

public key (PK) encryption type keys stored by SPU 500 and managed by key and tag

manager 558 may include, for example, a device public key, a device private key, a PK

certificate, and a public key for the certificate.) and (col. 164, lines 40-43; A key

identification number may be placed "in plain view" at the front of the records of secure

database 610 so the SPE 503 can determine which key to use the next time the record

is retrieved)

Regarding Claim 7, a secure processing unit as in claim 1, further comprising:

access control data, the access control data being operable to indicate whether access

to predefined (secure) memory regions is restricted to certain software components or

processor modes. (see col. 77, lines 43-48; Access Control List (ACL) structures, to

user and process defined events, including state transitions. ROS 602 may provide fill

control information over pre-defined and user-defined application events.)

Regarding Claim 8, a secure processing unit as in claim 7, in which the access

control data are stored in a critical address register, the critical address register

comprising one of the processor security registers. (see col. 121, lines 59-65;

Participants that receive appropriate permissions can register their processes (e.g.,

specific budgets) with summary services manager 560, which may then reserve

protected memory space (e.g., within NVRAM 534b) and keep desired use and/or

access parameters. Access to and modification of each summary can be controlled by

its own access tag.)

Regarding Claim 10, a secure processing unit as in claim 1, whereby level-two page tables that may not designate the predefined memory regions are not stored in the internal memory unit. (see col. 69, lines 43-47; Since the external memory may not be secure, SPU 500 may encrypt and cryptographically seal code and other information before storing it in external memory.)

Regarding Claim 11, an information appliance comprising:

a) a memory unit; (see col. 71, lines 7-10)

b) a secure processing unit (SPU) (see col. 79, lines 37-41) comprising

    (1) a tamper resistant packaging, (see col. 169, lines 28-31);

    (2) tamper detection and response logic, (see col. 169, lines 32-36);

    (3) a secure memory unit, and (see col. 65, lines 13-15);

    (4) a processing unit, (see col. 65, lines 13-15);

    (5) including a memory management unit (see col. 65, lines 15-20);

    (6) a plurality of processor security registers; (see col. 107, lines 25-26).

c) a level-one page table and a plurality of level-two page tables, the level-one page table including a plurality of level-one page table entries and the level-two page table including a plurality of level-two page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit

whether a corresponding level-two page table may designate certain predefined

(secure) memory regions; (see col. 69, lines 35-50)

d) a bus for connecting the memory unit and the secure processing unit; (see col.

62, lines 8-18; Bus 653 connects CPU(s) 654 to RAM 656, ROM 658, and I/O

controller 660. One or more SPUs 500 may also be connected to system bus

653. System bus 653 may permit SPU(s) 500 to communicate with CPU(s) 654,

and also may allow both the CPU(s) and the SPU(s) to communicate (e.g., over

shared address and data lines) with RAM 656, ROM 658 and I/O controller 660.)

wherein the secure processing unit is operable to perform *both* secure

processing operations and at least some processing operations performed by a

conventional information appliance processing unit. (see col. 80, lines 11-19;

Non-secure and secure HPE may operate together with a secure SPE.)

Regarding Claim 12, an information appliance as in claim 11, in which the information

appliance is selected from the group comprising: a television set-top box, a portable

audio player, a portable video player, a cellular telephone, a personal computer, and a

workstation. (see col. 61, lines 58-5; and col. 65, lines 3-10; SPU 500 may also be

integrated into other peripheral devices, such as CD-ROM devices, set-top cable

devices, game devices, and a wide variety of other electronic appliances that use,

allow access to, perform transactions related to, or consume, distributed information)

Regarding Claim 13, an information appliance as in claim 11, in which the secure

processing unit is the information appliance's *primary* processing unit. (see col. 63,

lines 23-26; Each VDE node or other electronic appliance 600 in the preferred

embodiment may include one or more SPUs 500. SPUs 500 may be used to perform

all secure processing for VDE 100.)

Regarding Claim 14, an information appliance as in claim 11, in which the secure

processing unit is the information appliance's *only* processing unit. (see col. 64, lines

42-46; SPU 500 may be integrated together with one or more other CPU(s) (e.g., a

CPU 654 of an electronic appliance) in a single component or package.)

Regarding Claim 15, an information appliance as in claim 11, in which the secure

processing unit includes:

a critical address register, the critical address register containing a plurality of access

control bits, the access control bits being operable to indicate whether access to

associated (secure) memory regions is restricted to predefined software components

or processor (protected) modes. (see col. 49, lines 40-44; a hardware SPU may

employ a host electronic appliance microcomputer operating in protected mode while

performing VDE related activities, thus allowing portions of VDE processes to execute

with a certain degree of security, and col. 275, lines 9-12; A VDE container is

associated with specific access control information and rights that are described in one

or more permissions control information sets (PERCs) associated with that container.

Regarding Claim 16, an information appliance as in claim 15, in which the critical

address register comprises one of the processor security registers. (see col. 179, lines

44-55; REGISTER method 2400 may then retrieve the administrative request from the

secure database and determine which response method to run to process the request)

Regarding Claim 18, an information appliance as in claim 11, in which level-two page tables that may not designate the predefined memory regions are stored in the memory unit, and wherein the level-one page table and the level-two page tables that may designate the predefined memory regions are stored in the secure memory unit. (see col. 69, lines 35-50; In these cases, secure processing steps performed by an SPU typically must be segmented into small, securely packaged elements that may be "paged in" and "paged out" of the limited available internal memory space. Memory external to an SPU 500 may not be secure. Since the external memory may not be secure, SPU 500 may encrypt and cryptographically seal code and other information before storing it in external memory. Similarly, SPU 500 must typically decrypt code and other information obtained from, external memory in encrypted form before processing (e.g., executing) based on it.)

Regarding Claim 19, in a system including a secure processing unit, the secure processing unit comprising an internal memory unit and a processor, and the processor including a memory management unit and a plurality of processor security registers, a method for controlling access to the internal memory unit, the method comprising:

a) obtaining a request to access a portion of memory in the internal memory unit; (see col. 69, lines 35-50)

b) checking critical address protection data stored in at least one of said processor security registers to determine whether the portion of memory is subject to critical access protection; (see col. 69, lines 35-50)

c) granting the request if the portion of memory is not subject to critical access protection. (see col. 69, lines 35-50)

Regarding Claim 20, a method as in claim 19, further including:

a) determining whether the processor is operating in a predefined (protected) mode; (see col. 49, lines 40-44; a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security)

b) granting the request if the processor is operating in the predefined (protected) mode. (see col. 49, lines 40-44; a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security)

Regarding Claim 21, a method as in claim 20, in which the predefined mode is a supervisor (protected) mode. (see col. 49, lines 40-44; a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security)

Conclusion

Prior Art

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a. U.S. Patent No. 6,292,569 to Shear et al. discloses Systems and methods using cryptography to protect secure computing environments.

    b. U.S. Patent No. 6,567,974 to Czajkowski discloses Small memory footprint system and method for separating applications within a single virtual machine.

Contact Information

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305-0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

    If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

    Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
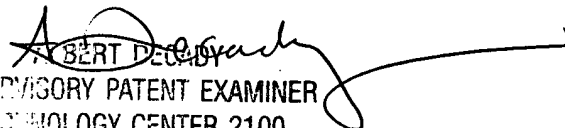
you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin
Patent Examiner
Art Unit 2132

KHS
March 28, 2004

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100